PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 20 AUG 2004
WIPO PCT

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
PCT 1897-03425		

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP 03/07829	18.07.2003	17.09.2002

International Patent Classification (IPC) or both national classification and IPC
H04L9/32

Applicant
PITSOS, Errikos

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 9 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
01.04.2004	20.08.2004

Name and mailing address of the international preliminary examining authority:

European Patent Office - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Authorized Officer

Dujardin, C

Telephone No. +31 70 340-2840

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/07829

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-38 as originally filed

Claims, Numbers

1-139 as originally filed

Drawings, Sheets

1/14-14/14 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees, the applicant has:

   ☐ restricted the claims.

   ☐ paid additional fees.

   ☐ paid additional fees under protest.

   ☒ neither restricted nor paid additional fees.

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

   ☐ complied with.

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

   ☐ all parts.

   ☒ the parts relating to claims Nos. 73-104 .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	73-104
	No:	Claims	
Inventive step (IS)	Yes:	Claims	73-104
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	73-104
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item IV

Lack of unity of invention

There are four inventions covered by the claims, indicated as follows:

1. Claims: 1-40
   Computing/obtaining the fingerprint of a list of fingerprints of digitally encoded data in a public key system.

2. Claims: 41-72
   Preventing cryptographic operations (encryption, decryption or signature) in a public key system by preventing the use of the private or of the public key of a first key pair and replacing the first key pair by a second key pair for executing the cryptographic operations.

3. Claims: 73-104
   Layered asymmetric encryption of digital data or layered digital signature of hashed digital data in a data distribution system.

4. Claims: 105-139
   Using the hash value of a random token and of a fixed random value as a key for symmetric encryption/decryption.

Document US6304974 represents the closest prior art. All features of claim 1 are disclosed in this document. All features of claim 2 to 12 are either disclosed in US6304974 or represent trivial improvements.

The problem solved by claim 13 is to determine whether the integrity of received fingerprints or first list of fingerprints has been compromised. The comparison of the computed fingerprint of a list of fingerprints with obtained first and second fingerprints of said list of fingerprints is the special technical feature of the first invention.

The problem solved by claims 41-72 is to control access to encrypted data selectively for different time periods and/or selectively for different users in a public key system. Preventing cryptographic operations by preventing the use of the private or of the public key of a first key pair and replacing the first key pair by a second key pair for executing the cryptographic operations are the potential special technical features of this second invention.

The problem solved by claims 73-104 is to distribute data securely in a public key system allowing several parties to jointly or sucessively encrypt and decrypt or to sign and verify the distributed digital data.
The layered asymmetric encryption of the digital data or the layered digital signature of the hashed digital data is the potential special technical feature of this third invention.

The problem solved by claims 105-139 is to use symmetric key information without the requirement to store this shared secret by the server for each user.
The use of a hash value of a random token and of a fixed random value as key information is the potential special technical feature of this fourth invention.

Consequently neither the problem underlying the subjects of the four claimed inventions, nor their solutions defined by the special technical features allow for a relationship to be establish between said inventions.

In conclusion, the four groups of claims are not linked by common or corresponding special technical features and define four different inventions not linked by a single general inventive concept. Hence, the application does not meet the requirements of unity of invention as defined in Rule 13(1) and (2) PCT.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The claims are not correctly drafted, which results in lack of clarity and lack of conciseness (**Article 6 PCT**):
    a) the application contains too many independent claims of the same category (method claims 73, 79, 90 and 96; storage medium claims 86, 79, 102 and 104);
    b) dependent claims 81 and 99 are identical;
    c) many dependent claims appear to have been defined with an incorrect category (claims 87, 88 and 103) and/or with an incorrect or unclear dependency reference (claims 95, 97, 98 and 103);
    d) claim 93 is defined as being dependent on one of claims 90 to 92, although its subject-matter does not include all the features of the claims to which it refers, one of these features being replaced by a different feature in claim 93.

2. Reference is made to the following document:
D1: WO 01/06702 A (POSTE ;FRANCE TELECOM (FR); REMERY PATRICK (FR); TRAORE JACQUES (F) 25 January 2001 (2001-01-25)

2.1. The document D1 (the references in parentheses applying to this document) is regarded as being the closest prior art to the subject-matter of independent claims 73 and 79 and shows a method (page 7, line 13 - page 8, line 12; page 11, lines 11-28), which can be considered as a method for providing a layered asymmetric encryption of digital data, in a data distribution system (like in claim 73) or as a method for controlling the distribution path of digital data from a sender to a recipient via a network (like in claim 79), and wherein the digital data is encrypted/decrypted according to a plurality of encryption layers and a plurality of corresponding keys (data encryption keys) successively and all the keys are distributed during an initialization phase (prior or parallel to the distribution of the digital data).

The subject-matter of claims 73 and 79 differs from this known method in that the digital data is encrypted/decrypted according to a single encryption layer using a first key (data encryption key), in that the first key is encrypted/decrypted according to a plurality of encryption layers and a plurality of corresponding keys (key encryption keys) successively and in that the encrypted first key is provided during the same phase as the encrypted data.

The subject-matter of claims 73 and 79 is therefore new (Article 33(2) PCT).

The twofold problem to be solved by the present invention may be regarded as allowing the use of a different data encryption key at each data transmission without the need for reinitializing the keys of all entities of the system or network and allowing the transport of the data encryption key without re-encrypting the encrypted data at each encryption layer.

The solution to the second part of this problem, proposed in claims 73 and 79 of the present application, is neither known nor suggested by the available prior art and is therefore considered as involving an inventive step (Article 33(3) PCT).

2.2. The document D1 is also regarded as being the closest prior art to the subject-matter of independent claims 90 and 96 and shows a method (page 7, line 13 - page 8, line 12; page 11, lines 11-28), which can be considered as a method

for controlling the distribution of digital data in a public key system using digital signatures on said digital data (like in claim 90) or as a method for controlling the distribution path of digital data from a sender to a recipient via a network (like in claim 96), and wherein the digital data is signed/verified according to a plurality of digital signature schemes (including the hashing of the data) and a plurality of corresponding key pairs successively.

The subject-matter of claims 90 and 96 differs from this known method in that the hash value of digital data is signed/verified according to a single digital signature scheme using a first key pair and in that the resulting first digital signature is signed/verified according to another digital signature scheme using another key pair.

The subject-matter of claims 90 and 96 is therefore new (Article 33(2) PCT).

The problem to be solved by the present invention may be regarded as transporting the signature of the (hashed) digital data without re-signing the complete message at each signature layer.

The solution to this problem proposed in claims 90 and 96 of the present application is neither known nor suggested by the available prior art and is therefore considered as involving an inventive step (Article 33(3) PCT).

2.3. Claims 74-78, 80-85, 91-95, 97-98 and 100-101 are dependent on claims 73, 79, 90 and 96 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

3.1. The independent claims 86, 79, 102 and 104 are the storage medium claims respectively corresponding to the method claims 83, 73-85, 101 and 90-101, whose subject-matter is new and inventive (see paragraph 2 above). Therefore the subject-matter of claims 86, 79, 102 and 104 is also new (Article 33(2) PCT) and involves an inventive step (Article 33(3) PCT).

3.2. Claims 87-88 and 103 are dependent on claims 86 and 102 and as such also meet the requirements of the PCT with respect to novelty and inventive step.